1. How to Use Nmap for Advanced Port Scans?

For **advanced port scans with Nmap**, you can use a range of specialized techniques to gain detailed information about open ports, services, and vulnerabilities on your target. Here's a breakdown of **advanced Nmap commands and options** for getting the most out of your scans:

---

1. SYN (Stealth) Scan

- **Command:** `nmap -sS <target>`
- **Purpose:** Performs a stealthy scan by only sending SYN packets, which initiates but does not complete a TCP handshake. It's faster and can evade certain detection.

2. TCP Connect Scan

- **Command:** `nmap -sT <target>`
- **Purpose:** Uses a full TCP handshake, making it easier to detect but useful for scanning networks where SYN scans may be restricted.

3. UDP Scan

- **Command:** `nmap -sU <target>`
- **Purpose:** Scans for open UDP ports (e.g., DNS, SNMP). UDP scans can be slow, so combine it with specific port ranges for faster results.

4. Service Version Detection

- **Command:** `nmap -sV <target>`
- **Purpose:** Determines the version of services running on open ports, which helps identify potential vulnerabilities.

5. OS Detection

- **Command:** `nmap -O <target>`
- **Purpose:** Analyzes network responses to identify the operating system of the target, including kernel version details.

6. Aggressive Scan

- **Command:** `nmap -A <target>`
- **Purpose:** Combines OS detection, version detection, and script scanning. Ideal for comprehensive scans but more detectable.

7. Specifying Port Ranges

- **Command:** `nmap -p 1-1000 <target>`

- **Purpose:** Focuses on specific ports or ranges, making the scan faster. You can also scan non-sequential ports like `-p 22,80,443`.

8. Timing Options

- **Command:** `nmap -T4 <target>`
- **Purpose:** Adjusts scan speed for stealth or speed:
  - `-T0` (Paranoid) – Very slow but stealthy.
  - `-T4` (Aggressive) – Fast, best for controlled environments.
  - `-T5` (Insane) – Fastest, very detectable.

9. Scan Using Nmap Scripting Engine (NSE)

- **Command:** `nmap --script <script> <target>`
- **Purpose:** NSE enables automation and customization for vulnerability detection, brute force attacks, malware discovery, and more. Some useful scripts:
  - `nmap --script vuln <target>` – Scans for known vulnerabilities.
  - `nmap --script http-enum <target>` – Identifies HTTP services and directories.

10. Scanning All Ports

- **Command:** `nmap -p- <target>`
- **Purpose:** Scans all 65,535 ports, revealing every open port. Best used with `-T4` or `-T5` in a lab or testing environment.

11. TCP SYN and UDP Combined Scan

- **Command:** `nmap -sS -sU -p T:22,80,443,U:53 <target>`
- **Purpose:** Runs a simultaneous scan on TCP and UDP ports, allowing detailed analysis of both protocols.

12. Scan and Output Results in Multiple Formats

- **Command:** `nmap -oN output.txt -oX output.xml -oG output.grep <target>`
- **Purpose:** Saves results in normal, XML, and grepable formats, which is ideal for reporting and automating follow-up actions.

13. Bypass Firewalls and IDS with Fragmentation

- **Command:** `nmap -f <target>`
- **Purpose:** Splits packets into smaller fragments, making it harder for intrusion detection systems (IDS) to detect.

Example Advanced Command for a Full Scan

```
nmap -sS -sV -O -p 1-1000 --script vuln -oN output.txt <target>
```

This command:

1. **Performs a SYN scan** (`-sS`),
2. **Detects service versions** (`-sV`),
3. **Identifies the operating system** (`-O`),
4. **Scans ports 1-1000** (`-p 1-1000`),
5. **Looks for vulnerabilities** (`--script vuln`),
6. **Saves the output** in a readable format (`-oN output.txt`).

Tips for Successful Advanced Scanning

- **Run Nmap with Sudo Privileges:** Some scans, like SYN and OS detection, require root privileges.
- **Limit Scope for Faster Scans:** Use specific ports, IP ranges, and timing settings.
- **Experiment with NSE Scripts:** The NSE library is vast and includes powerful scripts for specialized tasks.
- **Interpret Results Carefully:** Understanding open/closed/filtered ports, OS fingerprints, and NSE results is key to effective scans.